STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Mike Coffman
Secretary of State

Holly Z. Lowder
Director of Elections

Conditions for Use
Hart Voting System 6.2.1
August 26, 2008

The Testing Board recommends the following conditions for use of the voting system. The conditions for use shall be implemented by a county

Any deviation from the conditions provides significant weakness in the security, auditability, integrity and availability of the voting system.

Global Conditions (applies to all components):

1) Modem and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.

2) Provisional ballots must be processed separately from non-provisional ballots – system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.

3) Coordination of Escrow Setup - Upon Certification, voting system manufacturer must coordinate the escrow of the TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.

4) Abstract Report generation - abstracts used for State reporting must come from Tally Software, or other external solution, rather than from the specific device.

5) Trusted Build Verification

a) The system components do not allow for proper verification of trusted build software. Any breach of custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software components of the system. Additionally, due to concerns and previous history of software version control with this vendor, counties will be required to audit equipment and submit reports as necessary by the Secretary of State's office to ensure that only the approved components are present on any system in use in this state. Submission of this information shall happen at least once prior to each election and following each election.

b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of VSTL/EAC and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

6) Counties using the voting system shall affirm in their security plan submission that the voting system is used only on a closed network and/or as stand alone devices as required.

7) Use of wireless components is forbidden on the system. Any workstation or laptop that is designed with wireless communications shall have the device disabled and unable to be enabled by anyone other than the system administrator.

8) Election Programming and database distribution shall take place by one of the following three methods:

a) In the event the county has the software and technical expertise to confidently program their own election, the county shall submit any non-default template to the Secretary of State's office for verification prior to the download of memory cards used in the election. This effort will match the details prescribed under the ballot processing requirements for each device.

b) In the event the county has the software but not the expertise to program their own election, counties may choose to coordinate through the manufacturer or other third party company for this service. These companies must be bonded and insured as required under Secretary of State Rule 11. Copies of the database and separated template files must be submitted to the Secretary of State's office as indicated under the ballot processing requirements for each device. In addition, the counties must use the appropriate software to change administrator and device level passwords preventing the manufacturer from knowing such passwords.

c) In the event that the county does not have the software to program the election, the county may choose to coordinate through the manufacturer or other third party company for this service. These companies must be bonded and insured as required under Secretary of State Rule 11.

The county shall follow the following procedures to ensure the integrity of the trusted build and the verification of vote totals:

1. Counties shall log any deployment of a vendor to any voting location within the county (this includes pre-election testing, early voting and polling places).

a. Logs must contain the name of location, vendor name, county person name, date/time, and system serial number at a minimum.

2. Counties shall comply with accompaniment rule (43.8.6.1) for vendors having access to equipment to ensure that a vendor is accompanied at all times by a county employee.

3. Vendor is allowed any access to voting devices deemed necessary by county official.

a. Counties have the option to quarantine (Secure) the device and request backup equipment from SOS in lieu of vendor accessing voting device.

4. County shall conduct a 100% manual audit of the paper record of all races and ballots cast recorded by the device.

a. The MBB (Memory card) may be uploaded after audit is verified to match paper records.

b. If audit does not match, the device shall be quarantined (secured) and the county shall contact the SOS.

5. For any voting device handled by the voting system vendor, the trusted build shall be reinstalled after the election.

6. Counties shall submit logs and records of hand audits for devices that fall into this category prior to the canvass of official results to the Secretary of State.

All copies of the database and separated template files must be submitted to the Secretary of State's office as indicated under the ballot processing requirements for each device for the original database and any subsequent changes to the database.

Counties shall identify in the filing of their security plans which method will be executed for a given election.

Software Conditions (BOSS and Components):

1) System/Database/Network Security Hardening.

a) Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or request a variance from the Secretary of State to create Hart system hardening documentation in lieu of environmental changes. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.

b) In addition to physical environmental changes, counties shall maintain the integrity of the master Tally databases with one of the following two methods:

Option #1 - Create a second (or backup) copy of the BOSS, and in some cases, the Tally database that is created immediately after the point of memory card downloads. The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals and stored in a sealed or lockable transfer case that is stored in a limited access area. On Election Day, the designated election official shall load the sealed copy of the database onto the server/workstation, create a Tally database, if necessary, from the secured copy of the finalized database and proceed with uploading memory cards into Tally after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location;

OR

Option #2 - Create a second (or backup) copy of the BOSS database that is created immediately after the point of downloading all memory cards. The copy of the database will be escrowed with the Colorado Secretary of State's office along with the template files used. After each of the events described below, the county shall provide both an updated copy of the database to the Secretary of State's office, an updated database audit log, and the forensic analysis of the database performed by a commercially available forensics tool, identifying changes to database properties since the last report. Events triggering a report update to the Secretary of State include: any download of memory cards, any upload of memory cards, completion of L&A Testing, and completion of Post-Election Audit. Reports are to be submitted to the Secretary of State's office within 24 hours of the event.

Counties shall indicate in their Security Plan which option they will be executing to meet the security requirements.

c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased audits for this system. Counties shall verify results with one of two methods:

Option #1 – Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the Tally software. When memory cards are delivered to the county for upload, the machine generated

report shall be delivered for inspection as well. All reports generated shall remain with the memory card for verification purposes.;

OR

Option #2 – Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvass period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the software totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

2) Virus Protection.

The county shall submit for review to the Secretary of State a solution to virus protection that allows for manual updates as required.

3) Audit Trail Information:

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally or other software component for processing by other methods.

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

Such logs may be achievable by a manner best suitable to each county. Solutions may include the use of key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records or any combination to achieve the necessary audit data. Counties shall report to the Secretary of State's office through their security plans the method of achieving this condition.

4) Performance Deficiencies.

a) Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

b) Counties shall ensure that hardware purchased for use of the system matches the specifications of VSTL versions, not the Hart documentation.

5) Provisional Ballots.

The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirements of rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

6) Election Database Creation and Testing.

a) The system was unable to be fully tested with all Testing Board requirements for ballot layouts as required. Therefore, additional testing will be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

b) Counties to ensure ballots are designed and created according to state requirements. The vendor may offer a solution that includes non-certified and non-tested proprietary components. Counties may not use any modified template other than what is available as part of the default, and trusted configuration.

Precinct Count Scanner Conditions (eScan):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) Ballot Processing.

a) Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office and have been issued hash values by the Testing Board. Changes to template files must be submitted to the Secretary of State in the same manner as the original templates.

b) The device shall be set up so that the pollworker is required to use the override key on the back of the device in the event a ballot is rejected. Additionally each ballot or ballot page shall finish being fed through the eScan before the next ballot or ballot page is to be scanned.

3) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendors' recommendation for the component.

4) Device Security Accessibility.

a) County use of voting system will be required to modify the "administrator" password on the voting devices preventing the manufacturer access to the device by means of a password. Refer to Global Condition #8 for additional details on this condition and optional procedures to mitigate security concerns by this deficiency.

b) Counties shall coordinate with the vendor and submit to the state the plan for an approved transfer container for securing ballots after the close of polls on the device.

c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the Tally software as indicated in Software condition #1c.

5) Audit Trail Information:

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally software for processing by other methods.

b) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

c) Due to errors in processing and auditing information processed by the device, the device will be limited in functionality to only using serial numbered ballots.

d) Election official shall not reset the device without first creating an event and backing up the device in order to maintain a complete history of the audit logs.

6) Voting Secrecy.

Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from Hart) is used for ballots that are 14" in length or shorter. For

ballots outside of this description, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

Central Count Scanner Conditions (Ballot Now/Scanners):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) Ballot Processing.

a) Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office and have been issued hash values by the Testing Board. Changes to template files must be submitted to the Secretary of State in the same manner as the original templates

b) Counties shall manually resolve all races containing an overvote or a vote for a write-in candidate and shall be required to use AutoResolve for all undervotes when resolving ballot images.

3) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendors' recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.

4) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at minimum exporting results from the appropriate software module for processing by other methods.

c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amount of ballots counted on the device for the specific races selected in the post election audit:

Total # of Ballots Counted on Device	Total # of Ballots to Audit	# of Errors Requiring Escalation
150,000 to 500,000	1,250	6
35,001 to 150,000	800	4
10,001 to 35,000	500	3
3,201 to 10,000	315	2
1,201 to 3,200	200	2
501 to 1,200	125	2
281 to 500	80	1
151 to 280	50	1
91 to 150	32	1
51 to 90	20	1
26 to 50	13	1
16 to 25	8	1
9 to 15	5	1
1 to 8	3 or 100% if less than 3	1

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold. The verification of the hand count of paper ballots shall match the totals generated from the Tally software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

5) Network Access/Availability.

The voting system must be used with no network connectivity between devices/units and software. Only a direct connection (SCSI, IEEE 1394(i.e. Firewire), etc.) between scanner and workstation will be allowed.

DRE Conditions (eSlate):

1) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendors' recommendation for the component to accommodate a 120 minute short coming experienced by the Testing Board during testing of the device

2) Intrusion Seals for Protection of Trusted Build Firmware.

a) Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other

entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

b) Election official shall be required to change passwords for the JBC preventing the manufacturer to have access by means of password to the device. Refer to Global Condition #8 for additional details on this condition and optional procedures to mitigate security concerns by this deficiency.

3) Ballot Processing.

Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office, have been issued hash values by the Testing Board and have been included with the Trusted Build components of the voting system. Changes to template files must be on file as part of the trusted build in the same manner.

4) V-VPAT Paper Record Shall Be Handled Per Rule 11.6.

a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.

b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

5) Audit Trail Information:

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally software for processing by other methods.

b) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

c) Election official shall not reset the device without first creating an event and backing up the device in order to maintain a complete history of the audit logs.

6) V-VPAT Security.

a) The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT printer and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

b) The lock on the V-VPAT unit must be sealed with a tamper-evident seal.

7) Accessible Operation.

a) Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

b) A headset with an adjustable volume, which meets the State of Colorado specifications, must be provided.

8) V-VPAT Truncation

Due to space limitations on the paper tape, the V-VPAT may truncate lengthy candidate names. In order to mitigate this issue, during the conduct of Logic and Accuracy Testing counties shall determine whether or not truncation will occur. If there is any indication of truncation, printed notice will be provided to the voters prior to voting on the DRE.